

# AN APPLICATION OF THE SYMPLECTIC ARGUMENT TO SOME FERMAT-TYPE EQUATIONS

NUNO FREITAS AND ALAIN KRAUS

**ABSTRACT.** Let  $p$  be a prime number. In the early 2000s, it was proved that the Fermat equations with coefficients

$$3x^p + 8y^p + 21z^p = 0 \quad \text{and} \quad 3x^p + 4y^p + 5z^p = 0$$

do not admit non-trivial solutions for a set of exponents  $p$  with Dirichlet density  $1/4$  and  $1/8$ , respectively. In this note, using a recent criterion to decide if two elliptic curves over  $\mathbb{Q}$  with certain types of additive reduction at 2 have symplectically isomorphic  $p$ -torsion modules, we improve these densities to  $3/8$ .

**RÉSUMÉ.** **Une application du critère symplectique à quelques équations de Fermat.** Soit  $p$  un nombre premier. Au début des années 2000, il a été démontré que les équations de Fermat à coefficients

$$3x^p + 8y^p + 21z^p = 0 \quad \text{et} \quad 3x^p + 4y^p + 5z^p = 0$$

ne possèdent pas de solutions non triviales pour un ensemble d'exposants  $p$  de densité de Dirichlet  $1/4$  et  $1/8$ , respectivement. Dans cette note, en utilisant un résultat récent permettant de décider si deux courbes elliptiques sur  $\mathbb{Q}$ , ayant un certain type de réduction additive en 2, ont leurs modules des points de  $p$ -torsion symplectiquement isomorphes, on améliore ces densités à  $3/8$ .

## 1. INTRODUCTION

In [5] J.P.-Serre raised questions regarding specific instances of the *Fermat equation with coefficients*, that is

$$(1.1) \quad ax^p + by^p + cz^p = 0$$

where  $p$  is a prime and  $a, b, c \in \mathbb{Z}$  are fixed and non-zero.

In [3] the second author and Halberstadt introduced the *symplectic argument* as a complement to the modular method and partly solved the questions raised by Serre, together with other instances of the equation above. Indeed, for some explicit choices of  $a, b$  and  $c$  they used Theorem 4 below and [3, Lemma 1.7] to show that (1.1) does not have solutions when the exponent  $p$  belongs to certain congruence classes. Another diophantine application of the symplectic argument and Theorem 4 can be found in [2], where it was used to solve the classical Fermat equation over  $\mathbb{Q}(\sqrt{17})$  for a set of exponents with density  $1/2$ .

We remark that the reason why the symplectic argument is necessary is invisible in the proof of Fermat's Last Theorem where the modular method has its origin. Indeed, after applying

---

2010 *Mathematics Subject Classification.* Primary 11D41, Secondary 11G07.

*Key words and phrases.* Fermat equations, elliptic curves, symplectic isomorphism.

modularity and level lowering results, one gets an isomorphism

$$\overline{\rho}_{E,p} \sim \overline{\rho}_{f,p}$$

between the mod  $p$  representations attached to the Frey curve and some newform  $f$  with weight 2 and ‘small’ level  $N$ . In the proof of FLT we have  $N = 2$  and there are no candidate newforms  $f$ , giving a contradiction. In essentially every other application of the modular method there are candidates for  $f$ , therefore more work is needed to obtain a contradiction to the previous isomorphism. The symplectic argument is a tool that allows to obtain the desired contradiction in certain cases. In particular, in the recent work [1] the first author proved a new symplectic criterion (Theorem 3 below) and used it to solve the Generalized Fermat equation  $x^3 + y^3 = z^p$  when  $(-3/p) = -1$ .

The purpose of this note is to further illustrate the strength of the symplectic argument, by combining the new and old criteria to improve two results originally obtained in [3]. More precisely, we will establish the following theorems.

**Theorem 1.** *Let  $p > 7$  be a prime satisfying*

$$p \equiv 5 \pmod{8} \quad \text{or} \quad p \equiv 23 \pmod{24}.$$

*Then the Fermat equation*

$$(1.2) \quad 3x^p + 8y^p + 21z^p = 0$$

*has no solutions  $(x, y, z) \neq (0, 0, 0)$ .*

**Theorem 2.** *Let  $p \geq 5$  be a prime satisfying*

$$p \equiv 5 \pmod{8} \quad \text{or} \quad p \equiv 19 \pmod{24}.$$

*Then the Fermat equation*

$$(1.3) \quad 3x^p + 4y^p + 5z^p = 0$$

*has no solutions  $(x, y, z) \neq (0, 0, 0)$ .*

Let us mention that the coefficients  $a, b, c$  of the Fermat equations (1.2) and (1.3) do not satisfy non-trivial linear relations with coefficients in  $\{-1, 0, 1\}$ . Conjecturally, we expect that for any prime number  $p$  large enough, the two equations have at least one local obstruction i.e. there is at least a prime number  $\ell$  such that they have no solutions over  $\mathbb{Q}_\ell$  (see [3, Conjecture (C)]). Indeed, such is the case for  $11 \leq p < 10^5$ . For  $p = 3$ , the curve of equation  $3x^p + 8y^p + 21z^p = 0$  has no points over  $\mathbb{Q}_3$  and  $\mathbb{Q}_7$ ; for  $p = 5$  and  $p = 7$ , it has no local obstructions. The curve of equation  $3x^p + 4y^p + 5z^p = 0$  has no local obstruction for  $p = 3$ ; for  $p = 5$  it has no points over  $\mathbb{Q}_{11}$  and for  $p = 7$  it has no points over  $\mathbb{Q}_{29}$  and  $\mathbb{Q}_{43}$ . Moreover, if  $k$  is a fixed positive even integer, for any  $p$  large enough such that  $q = kp + 1$  is prime, the curves have a local obstruction at  $q$  (see Proposition 3.3 in *loc. cit.*). For example, with  $k = 2$  such is the case as soon as  $p \geq 11$ .

## 2. TWO SYMPLECTIC CRITERIA

In this section we state the criteria we will use in the proofs. We first recall some terminology.

Let  $E, E'$  be elliptic curves over  $\mathbb{Q}$  with  $p$ -torsion modules  $E[p], E'[p]$  and Weil pairings  $e_{E,p}, e_{E',p}$ , respectively. Let  $\phi : E[p] \rightarrow E'[p]$  be an isomorphism of  $G_{\mathbb{Q}}$ -modules. Then there is an element  $r(\phi) \in \mathbb{F}_p^\times$  such that

$$e_{E',p}(\phi(P), \phi(Q)) = e_{E,p}(P, Q)^{r(\phi)} \quad \text{for all } P, Q \in E[p].$$

Note that for any  $a \in \mathbb{F}_p^\times$  we have  $r(a\phi) = a^2 r(\phi)$ . We say that  $\phi$  is a *symplectic isomorphism* if  $r(\phi) = 1$  or, more generally,  $r(\phi)$  is a square in  $\mathbb{F}_p^\times$ . Fix a non-square  $r_p \in \mathbb{F}_p^\times$ . We say that  $\phi$  is a *anti-symplectic isomorphism* if  $r(\phi) = r_p$  or, more generally,  $r(\phi)$  is a non-square in  $\mathbb{F}_p^\times$ . Finally, we say that  $E[p]$  and  $E'[p]$  are *symplectically* (or *anti-symplectically*) *isomorphic*, if there exists a symplectic (or anti-symplectic) isomorphism of  $G_{\mathbb{Q}}$ -modules between them.

The following is [1, Theorem 3].

**Theorem 3.** *Let  $E/\mathbb{Q}_2$  and  $E'/\mathbb{Q}_2$  be elliptic curves with potentially good reduction. Write  $L = \mathbb{Q}_2^{un}(E[p])$  and  $L' = \mathbb{Q}_2^{un}(E'[p])$ . Write  $\Delta_m(E)$  and  $\Delta_m(E')$  for the minimal discriminant of  $E$  and  $E'$  respectively. Let  $I_2 \subset \text{Gal}(\overline{\mathbb{Q}_2}/\mathbb{Q}_2)$  be the inertia group.*

*Suppose that  $L = L'$  and  $\text{Gal}(L/\mathbb{Q}_2^{un}) \simeq \text{SL}_2(\mathbb{F}_3)$ . Then,  $E[p]$  and  $E'[p]$  are isomorphic  $I_2$ -modules for all prime  $p \geq 3$ . Moreover,*

- (1) *if  $(2/p) = 1$  then  $E[p]$  and  $E'[p]$  are symplectically isomorphic  $I_2$ -modules.*
- (2) *if  $(2/p) = -1$  then  $E[p]$  and  $E'[p]$  are symplectically isomorphic  $I_2$ -modules if and only if  $v_2(\Delta_m(E)) \equiv v_2(\Delta_m(E')) \pmod{3}$ .*

*Furthermore,  $E[p]$  and  $E'[p]$  cannot be both symplectic and anti-symplectic isomorphic  $I_2$ -modules.*

The following is [4, Proposition 2].

**Theorem 4.** *Let  $E, E'$  be elliptic curves over  $\mathbb{Q}$  with minimal discriminants  $\Delta, \Delta'$ . Let  $p$  be a prime such that  $\overline{\rho}_{E,p} \simeq \overline{\rho}_{E',p}$ . Suppose that  $E$  and  $E'$  have multiplicative reduction at a prime  $\ell \neq p$  and that  $p \nmid v_\ell(\Delta)$ . Then  $p \nmid v_\ell(\Delta')$ , and the representations  $\overline{\rho}_{E,p}$  and  $\overline{\rho}_{E',p}$  are symplectically isomorphic if and only if  $v_\ell(\Delta)/v_\ell(\Delta')$  is a square mod  $p$ .*

## 3. PROOF OF THEOREM 1

Suppose  $(x, y, z)$  is a non-trivial primitive solution to (1.2). From [3, Example 2.5] we know that the Frey curve  $E_{x,y,z}$  attached to  $(x, y, z)$  has minimal discriminant  $\Delta_{x,y,z}$  given by

$$\Delta_{x,y,z} = \begin{cases} 2^{10} \cdot 3^{2p-2} \cdot 7^2 \cdot (xyz)^{2p} & \text{if } y \text{ is odd} \\ 2^{-2} \cdot 3^{2p-2} \cdot 7^2 \cdot (xyz)^{2p} & \text{if } y \text{ is even.} \end{cases}$$

Moreover, after applying the now classical modularity, irreducibility and level lowering results over  $\mathbb{Q}$  we conclude that

$$\overline{\rho}_{E_{x,y,z},p} \sim \overline{\rho}_{f,p}$$

where  $f$  is a newform for  $\Gamma_0(N)$  and weight 2 with level  $N$  given by

$$N = \begin{cases} 168 & \text{if } y \text{ is odd} \\ 42 & \text{if } y \text{ is even.} \end{cases}$$

There is only one such newform at level 42 and two of them at level 168. The three have rational coefficients hence correspond to isogeny classes of elliptic curves. We note that the curves in the isogeny class with Cremona label ‘42a’ have multiplicative reduction at 2 while the curves of conductor 168 have potentially good reduction at 2. Furthermore, their minimal extension  $L/\mathbb{Q}_2^{un}$  of good reduction satisfies  $\text{Gal}(L/\mathbb{Q}_2^{un}) \simeq \text{SL}_2(\mathbb{F}_3)$ .

We now divide the proof into two natural cases.

Case I: Suppose  $y$  is even. Thus  $E_{x,y,z}[p] \simeq E[p]$ , where  $E = 42a1$ . It is proved in [3, Example 2.5] that we get a contradiction with  $(-2/p) = -1$ .

Case II: Suppose  $y$  is odd. There is an isomorphism  $\phi : E_{x,y,z}[p] \simeq E[p]$ , where

$$E = 168a1, \quad \Delta_E = 2^4 \cdot 3 \cdot 7 \quad \text{or} \quad E = 168b1, \quad \Delta_E = -2^4 \cdot 3^3 \cdot 7^4.$$

Note that

$$v_2(\Delta_{x,y,z}) = 10, \quad v_3(\Delta_{x,y,z}) \equiv -2, \quad v_7(\Delta_{x,y,z}) \equiv 2,$$

where the congruences are mod  $p$ .

Suppose  $(2/p) = -1$  and  $E = 168a1$ . It follows from Theorem 1 that  $\phi$  is symplectic. Thus Theorem 4 implies that  $v_7(\Delta_{x,y,z})/v_7(\Delta_E) \equiv 2$  is a square mod  $p$ , a contradiction.

Suppose  $(2/p) = -1$  and  $E = 168b1$ . It follows from Theorem 1 that  $\phi$  is symplectic. Thus Theorem 4 implies that  $v_7(\Delta_{x,y,z})/v_7(\Delta_E) \equiv 2/4$  is a square mod  $p$ , a contradiction.

Suppose  $(2/p) = 1$  and  $E = 168a1$ . It follows from Theorem 1 that  $\phi$  is symplectic. Thus Theorem 4 implies that  $v_3(\Delta_{x,y,z})/v_3(\Delta_E) \equiv -2$  is a square mod  $p$ . This implies  $(-1/p) = 1$ .

Suppose  $(2/p) = 1$  and  $E = 168b1$ . It follows from Theorem 1 that  $\phi$  is symplectic. Thus Theorem 4 implies that  $v_3(\Delta_{x,y,z})/v_3(\Delta_E) \equiv -2/3$  is a square mod  $p$ . This implies  $(-3/p) = 1$ .

We therefore obtain a contradiction for all  $y$  if one of the following holds

- $(-2/p) = -1$  and  $(2/p) = -1$  or,
- $(-2/p) = -1$  and  $(2/p) = (3/p) = 1$

which represents the set of primes, with density  $3/8$ , in the statement of the Theorem 1.

#### 4. PROOF OF THEOREM 2

Suppose  $(x, y, z)$  is a non-trivial primitive solution to (1.3). From [3, Proposition 2.3] and its proof we know that the Frey curve  $E_{x,y,z}$  attached to  $(x, y, z)$  has minimal discriminant  $\Delta_{x,y,z}$  given by

$$\Delta_{x,y,z} = \begin{cases} 2^8 \cdot 3^2 \cdot 5^2 \cdot (xyz)^{2p} & \text{if } y \text{ is odd} \\ 2^{-4} \cdot 3^2 \cdot 5^2 \cdot (xyz)^{2p} & \text{if } y \text{ is even.} \end{cases}$$

Moreover, after applying the now classical modularity, irreducibility and level lowering results over  $\mathbb{Q}$  we conclude that  $\bar{\rho}_{E_{x,y,z},p} \sim \bar{\rho}_{f,p}$  where  $f$  is a newform for  $\Gamma_0(N)$  and weight 2 with level  $N$  given by

$$N = \begin{cases} 120 & \text{if } y \text{ is odd} \\ 30 & \text{if } y \text{ is even.} \end{cases}$$

There is only one such newform at level 30 and two of them at level 120, each corresponding to an isogeny class of elliptic curves. Note that the curves in the isogeny class with Cremona label ‘30a’ have multiplicative reduction at 2 while the curves of conductor 120 have potentially good reduction at 2. Furthermore, their minimal extension  $L/\mathbb{Q}_2^{un}$  of good reduction satisfies  $\text{Gal}(L/\mathbb{Q}_2^{un}) \simeq \text{SL}_2(\mathbb{F}_3)$ .

We now divide the proof into two natural cases.

CASE I: Suppose  $y$  is even. Thus  $E_{x,y,z}[p] \simeq E[p]$ , where

$$E = 30a1, \quad \Delta_E = -2^4 3^3 5^2.$$

From Theorem 2 the integers

- $v_2(\Delta_{x,y,z})v_3(\Delta_{x,y,z})$  and  $v_2(\Delta_E)v_3(\Delta_E)$ ,
- $v_2(\Delta_{x,y,z})v_5(\Delta_{x,y,z})$  and  $v_2(\Delta_E)v_5(\Delta_E)$ ,
- $v_3(\Delta_{x,y,z})v_5(\Delta_{x,y,z})$  and  $v_3(\Delta_E)v_5(\Delta_E)$ ,

must differ by multiplication by a square mod  $p$ . This gives a contradiction with

$$(-2/p) = -1 \quad \text{or} \quad (3/p) = -1.$$

CASE II: Suppose  $y$  is odd. Thus  $\phi : E_{x,y,z}[p] \simeq E[p]$ , where

$$E = 120a1, \quad \Delta_E = 2^4 \cdot 3^2 \cdot 5 \quad \text{or} \quad E = 120b1, \quad \Delta_E = -2^8 \cdot 3 \cdot 5.$$

Note that  $v_2(\Delta_{x,y,z}) = 8$  and  $v_3(\Delta_{x,y,z}) \equiv v_5(\Delta_{x,y,z}) \equiv 2 \pmod{p}$ .

Suppose  $(2/p) = -1$  and  $E = 120a1$ . It follows from Theorem 1 that  $\phi$  is anti-symplectic. Thus Theorem 4 implies that  $v_3(\Delta_{x,y,z})/v_3(\Delta_E) \equiv 1$  is not a square mod  $p$ , a contradiction.

Suppose  $(2/p) = -1$  and  $E = 120b1$ . It follows from Theorem 1 that  $\phi$  is symplectic. Thus Theorem 4 implies that  $v_5(\Delta_{x,y,z})/v_5(\Delta_E) \equiv 2$  is a square mod  $p$ , a contradiction.

For the case  $(2/p) = 1$  we cannot find further restrictions.

We therefore obtain a contradiction for all  $y$  if one of the following holds

- $(2/p) = -1$  and  $(-2/p) = -1$ ,
- $(2/p) = -1$  and  $(3/p) = -1$ .

The condition  $(2/p) = -1$  means  $p \equiv 3, 8 \pmod{5}$ ; if  $p \equiv 5 \pmod{8}$  we have  $(-2/p) = -1$  and the result follows in this case. Suppose  $p \equiv 3 \pmod{8}$ , hence  $(-2/p) = 1$ . Now the condition  $(3/p) = -1$  implies  $p \equiv 1 \pmod{3}$ . We get  $p \equiv 19 \pmod{24}$ , as desired. So we can conclude for a set of primes with density  $3/8$ .

## REFERENCES

- [1] N. Freitas, *On the Fermat-type equation  $x^3 + y^3 = z^p$* , Commentarii Mathematici Helvetici. To appear. [1](#), [2](#)
- [2] N. Freitas and S. Siksek, *Fermat's Last Theorem over some small real quadratic fields*, Algebra Number Theory **9** (2015), no. 4, 875–895. [1](#)
- [3] E. Halberstadt and A. Kraus, *Courbes de Fermat: résultats et problèmes*, J. Reine Angew. Math. **548** (2002), 167–234. [1](#), [1](#), [3](#), [4](#)
- [4] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275 [2](#)
- [5] J.-P. Serre, *Sur les représentations modulaires de degré 2 de  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Math. J. **54** (1987), 179–230. [1](#)

UNIVERSITY OF BRITISH COLUMBIA, DEPARTMENT OF MATHEMATICS, VANCOUVER, BC V6T 1Z2 CANADA

*E-mail address:* `nunobfreitas@gmail.com`

UNIVERSITÉ PIERRE ET MARIE CURIE - PARIS 6, INSTITUT DE MATHÉMATIQUES DE JUSSIEU, 4 PLACE JUSSIEU, 75005 PARIS, FRANCE

*E-mail address:* `alain.kraus@imj-prg.fr`